УДК 004.415.24

І.В. Швідченко
Інститут кібернетики імені В.М. Глушкова НАН України, м. Київ
Україна, 03187, м. Київ, проспект Академіка Глушкова, 40

Аналіз програмного забезпечення зі стеганоаналізу

I.V. Shvidchenko
Glushkov Institute of Cybernetics of National Academy of Sciences of Ukraine, c. Kyiv
Ukraine, 03187, c. Kyiv, Glushkova ave., 40

Investigation of Steganalysis Software

И.В. Швидченко
Институт кибернетики имени В.М. Глушкова НАН Украины, г. Киев
Украина, 03187, г. Киев, проспект Академика Глушкова, 40

Анализ програмного обеспечения по стеганоанализу

Стаття присвячена дослідженню й аналізу існуючих програм зі стеганоаналізу. Доведена необхідність розробки програмного комплексу, спрямованого на пошук, виявлення і вилучення прихованої інформації, контроль використання стенографічних алгоритмів.
Ключові слова: захист інформації, стеганографія, стеганоаналіз, прихована передача даних, контейнер, повідомлення.

The article is devoted to the investigation and analysis of current programs for steganoanalysis. Need for program complex development of search, detection and loading of hidden information as well as for control of stenographic algorithms use is proved.
Key words: information protection, steganography, steganalysis, hidden data transfer, cover medium, message.

Статья посвящена исследованию и анализу существующих программ по стеганоанализу. Доказана необходимость разработки программного комплекса, направленного на поиск, выявление и изъятие скрытой информации, контроль использования стенографических алгоритмов.
Ключевые слова: защита информации, стеганография, стеганоанализ, скрытая передача данных, контейнер, сообщение.

Вступ

Поширення комп’ютерної техніки і глобальних комп’ютерних мереж, простота в експлуатації обладнання (цифровими пристроями) і доступність для користувача безкоштовного або умовно-безкоштовного стеганографічного програмного забезпечення дозволяють сьогодні кожному бажаючому використовувати методи стеганографії при передачі інформації. Цими методами з легкістю може скористатися і зловмисник – протиборча сторона, яка намагається порушити безпеку інформації. Фахівцям, які працюють у сфері комп’ютерної безпеки, правоохоронних органах і розвідувальних службах, необхідно мати можливість виявляти стеганографічне приховання інформації, яка передається по відкритим каналам зв’язку. Таким чином, на сьогодні існує великий інтерес до стеганоаналізу. Стеганоаналіз – наука про вивчення методів виявлення існування секретної інформації у відкритих повідомленнях [1].

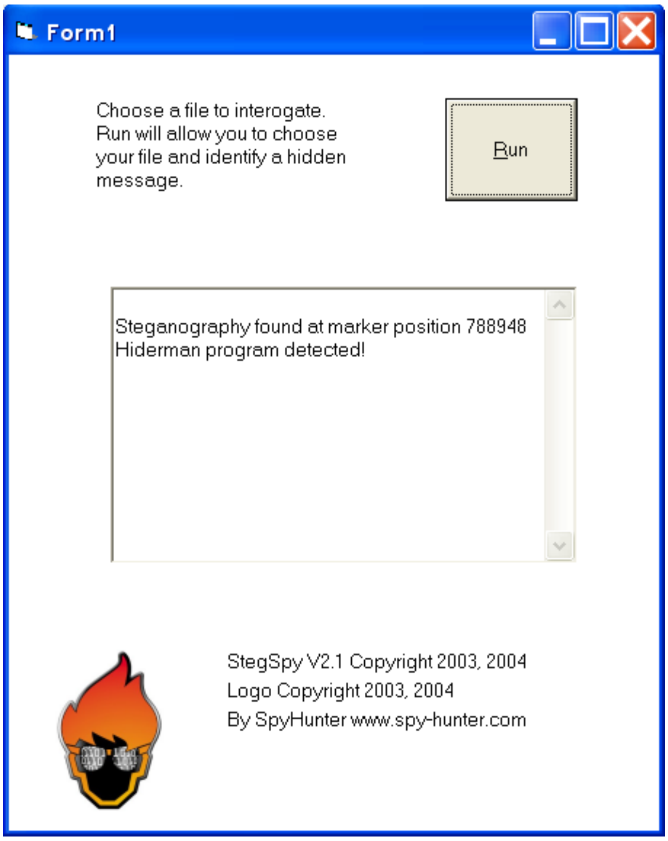
Виявлення прихованої передачі даних, прихованих одним із багатьох існуючих методів стеганографії в різні формати контейнерів, є досить складним процесом,

який неможливий без застосування сучасних інструментів [2], [3]. На сторінках російськомовного та україномовного Інтернету знайти будь-яку програму, що працює для стеганоаналізу, виявилось неможливим. Зазначимо, що відсутність доступного широкому загалу дослідників ефективних засобів розв'язання задач стеганоаналізу приводить до зростання застосування стеганографії в протиправній діяльності. У світі ця ситуація виглядає по-іншому. Зарубіжні веб-сайти пропонують програмне забезпечення з різними ліцензійними вимогами, яке дозволяє вирішити задачу стеганоаналізу – встановлення факту існування в контейнері прихованої інформації. Опишемо і проаналізуємо п'ять стеганоаналітичних програм, знайдених нами в мережі Інтернет.

StegSpy v2.1

StegSpy v2.1 (http://www.spy-hunter.com) – вільно поширюване програмне забезпечення зі стеганоаналізу, розроблене Michael T. Raggo. Програма виявляє існування інформації, прихованої за допомогою певних стеганографічних програм, таких як: Hiderman, JPHide and Seek, Masker, JPegX, Invisible Secrets. Поточна версія програми також визначає й місцезнаходження вкрапленої інформації. StegSpy v2.1 була представлена автором на конференціях InfoSec 2004, BlackHat 2004 й DefCon 2004.

StegSpy v2.1 написана мовою Visual Basic. Графічний інтерфейс програми (рис. 1 *а*) дозволяє користувачу вибирати файл-контейнер, який необхідно перевірити на наявність вкраплених даних.



а

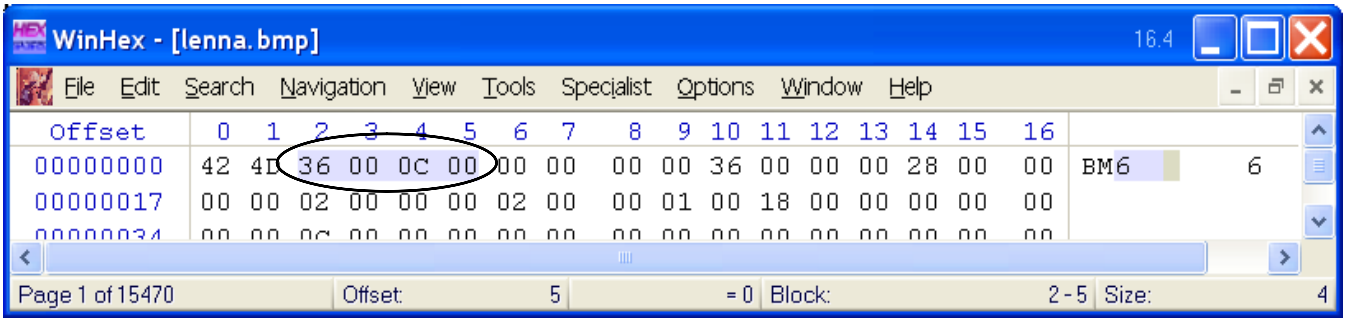


б

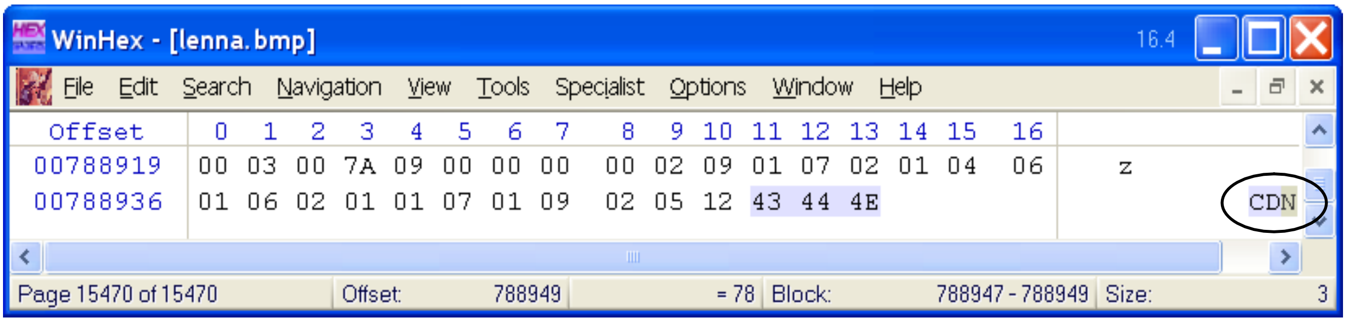
Рисунок 1 – *а* – зовнішній вигляд програми StegSpy v2.1,
б – стеганоконтейнер lenna.bmp

Щоб проаналізувати роботу програми StegSpy v2.1, був обраний файл у форматі *.bmp (рис. 1 *б*), в який було вкраплено текстове повідомлення з використанням стеганографічного додатка Hiderman. Як видно з рис. 1 *а*, програма з успіхом виявила наявність прихованої інформації, вкрапленої за допомогою цього додатка, починаючи з позиції 788948.

Відомо, що заголовок *.bmp файлу містить поле, яке вказує на розмір файла. На рис. 2 зображені верхні й нижні частини зображення в шістнадцятирічному редакторі. Заголовок файлу lenna.bmp (рис. 2 *а*) вказує, що його розмір дорівнює 786486 (00 0C 00 36) байт. Однак дані наприкінці заголовка (рис. 2 *б*) відображають розмір 788950 байт, що свідчить про наявність іншої інформації, прикріпленої до файла. Видно рядок “CDN”. Цей рядок завжди присутній при використанні стеганографічного додатка Hiderman. CDN – сигнатура Hiderman, і використовується StegSpy v2.1, щоб виявити стеганографічне програмне забезпечення, яке використовувалося для вкраплення повідомлення.



а



б

Рисунок 2 – Перегляд зображення в шістнадцятирічному редакторі:
а – початок заголовка файла lenna.bmp, *б* – кінець файла

Посилаючись на автора [4], StegSpy v2.1 використовує сигнатурні методи стеганоаналізу. Сигнатурні методи виконують пошук бітових послідовностей, специфічні для певних стеганографічних програм. Проте, змінюючи, наприклад, сигнатуру “CDN” на “000”, StegSpy v2.1, не в змозі виявити стеганографічне приховання в зображенні *.bmp. Таким чином, StegSpy v2.1 покладається тільки на сигнатуру файла й ігнорує виявлення аномалій файла. Тому після виявлення відомої сигнатури бажано переглянути файл в шістнадцятирічному редакторі, щоб визначити місце розташування позиції вкраплених даних, наприклад, виявляючи кінець зображення, який базується на інформації заголовка.

Недоліки:

1. Не дуже зручний графічний інтерфейс. StegSpy v2.1 проводить аналіз лише одного файла і не підтримує аналіз для набору файлів.
2. StegSpy v2.1 виявляє наявність вкраплених даних, прихованих однією з апріорно відомих стеганографічних програм, і тільки в тих форматах файлів, які ці програми підтримують.
3. StegSpy v2.1 використовує тільки сигнатурний метод, не підтримує методи, які базуються на виявленні аномалій файла.
4. Програма не вдосконалювалася з 2004 року.

Stegdetect 0.6

Stegdetect 0.6 (http://www.outguess.org/) – програмне забезпечення з відкритим програмним кодом для автоматичного виявлення застосування стеганографії в зображеннях. Розробником програми є Niels Provos [5]. Програма здатна виявляти декілька різних стеганографічних методів, які застосовуються для приховування інформації в JPEG зображеннях. Поточна версія виявляє наявність прихованих даних, які були вкраплені такими стеганографічними програмами, як Jsteg, Jphide (Unix та Windows), Invisible Secrets, Outguess 0.13b, F5 (Header Analysis), appendX та Camouflage.

На рис. 3 наведений графічний інтерфейс програми – Xsteg, при дослідженні двох файлів, пустого контейнера й контейнера, який містить приховані дані у форматі JPEG. Програма Stegdetect 0.6 не тільки виявляє наявність прихованих даних у файлі-контейнері, але і правильно припускає використовувану стеганографічну програму – JPHide.

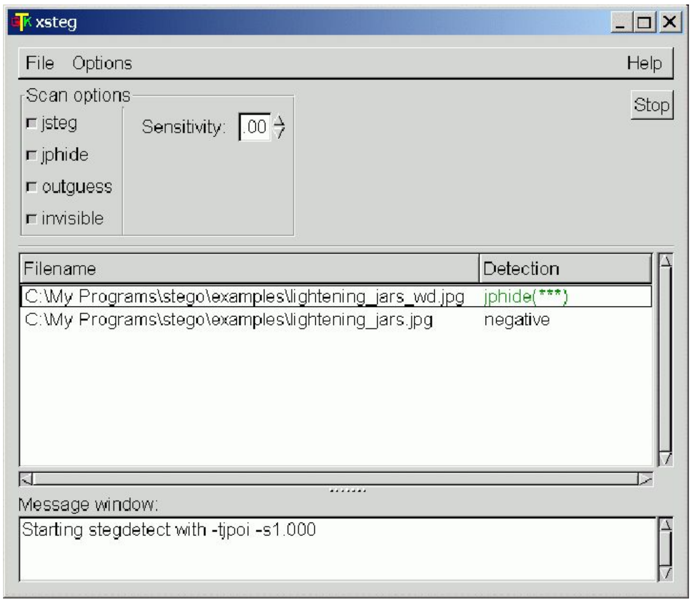


Рисунок 3 – Зовнішній вигляд програми Stegdetect

Stegdetect 0.6 в першу чергу перевіряє поля-коментарі й поля розширень різних форматів файлів, наявність штучно створених зображень, а також зображень із великою кількістю монотонних областей. Програма порівнює частоту розподілу кольорів для можливого носія прихованої інформації й теоретично очікувану частоту розподілу кольорів для файла-носія прихованої інформації. Stegdetect 0.6 показує гарні результати в тому випадку, якщо вміст вкрапленої інформації перевищує 10% від обсягу файла-контейнера.

Stegdetect 0.6 підтримує аналіз лінійного дискримінанта. З набору пустих зображень і набору зображень, які містять вкраплену інформацію, приховану одним із стеганографічних методів, Stegdetect 0.6 може автоматично визначити лінійну функцію виявлення, яка може бути застосована до некласифікованих зображень.

Аналізом лінійного дискримінанта обчислюється розділювальна гіперплощина, що відокремлює пусті контейнери від стеганоконтейнерів. Гіперплощина характеризується як лінійна функція. Досліджувана функція може бути збережена для подальшого використання в нових зображеннях.

Stegdetect 0.6 підтримує декілька різних функцій векторів й автоматично обчислює одержувані характеристики управління, які можуть бути використані для оцінки якості автоматично досліджуваної функції виявлення [6], [7].

Супутня Stegdetect 0.6 програма Stegbreak використовується для запуску атак «перебором за словником» проти JSteg-Shell, JPHide and OutGuess 0.13b.

Недоліки:

1. Підтримує тільки виявлення інформації в JPEG файлах.

2. Stegdetect 0.6 виявляє наявність вкраплених даних, прихованих однією з апріорно відомих стеганографічних програм.

3. Програма не вдосконалювалася з 2001 року.

XstegSecret beta v0.1

XstegSecret beta v0.1 (http://stegsecret.sourceforge.net) – відкритий проект зі стеганоаналізу, мета якого спрямована на збір, реалізацію і полегшення використання різних стеганоаналітичних методів, застосовних до цифрових медіа-файлів, таких як зображення, аудіо й відео. Розробником є іспанський дослідник Alfonso Muñoz. Програма має загальну публічну ліцензію General Public License (GNU). Графічний інтерфейс програми написаний іспанською мовою, але для пересічного користувача є інтуїтивно зрозумілим.

Програма надає можливість спочатку виконати сканування всієї файлової системи або окремих тек досліджуваних носіїв на наявність файлів-артефактів, які можуть бути асоційовані з окремим стеганографічним додатком. Програма містить базу даних BDAS v0.1, яка ідентифікує більше 40 стеганографічних програм (рис. 4).

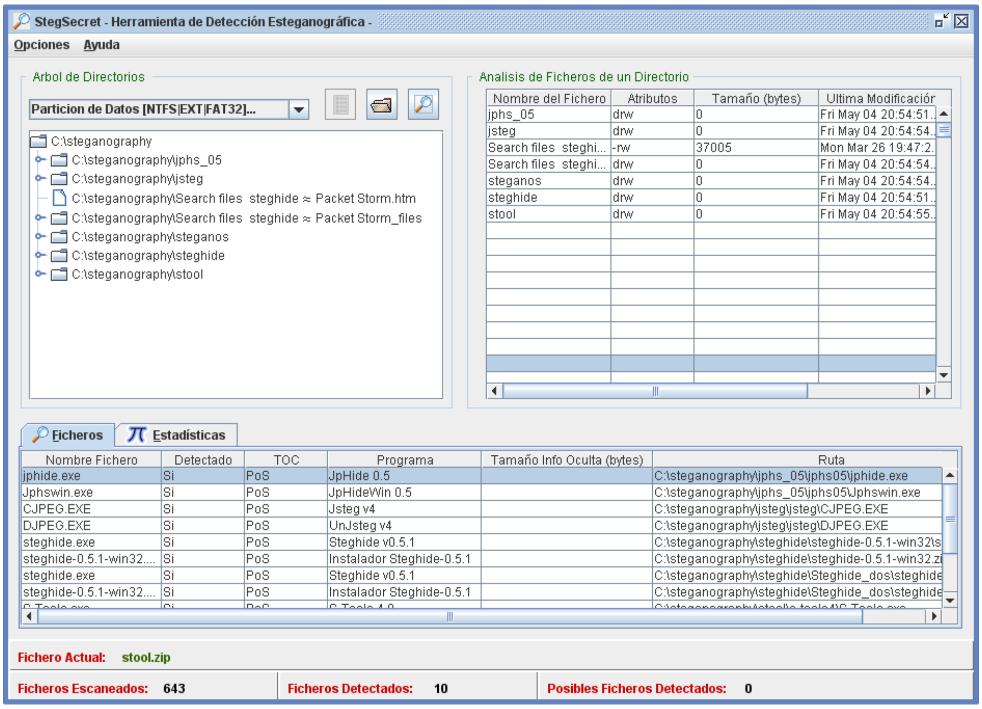


Рисунок 4 – Зовнішній вигляд програми XstegSecret beta v0.1:
процедура виявлення стеганографічних програм в теці, яка досліджується

Після того, як цифровий стеганографічний додаток виявлено, існує можливість виявити файли, які, можливо, були використані як стеганоконтейнери.

XstegSecret beta v0.1 виявляє інформацію, приховану за допомогою таких програм, як Camouflage V1.2.1, inThePicture v2, JPEGXv2.1.1, PGE (Pretty Good Envelope) v1.0, appendX v<=4, steganography v1.6.5, inPlainView, DataStash v1.5 та dataStealth v1.0. Для виявлення прихованої інформації програма використовує візуальний, структурний та статистичні методи стеганоаналізу (метод χ^2 та RS-стегано-аналіз).

Візуальні методи базуються на здатності зорової системи людини аналізувати зорові образи і виявляти істотні відмінності в зображеннях, що порівнюються. Основна ідея методу візуального аналізу бітових площин полягає в порівнянні зображення в цілому із зображеннями його бітових площин. XstegSecret beta v0.1 дає можливість розкласти зображення на його індивідуальні бітові площини (рис. 5). Бітова площина складається з одного біта пам'яті для кожного пікселя в зображенні і є типовим місцем зберігання інформації, прихованої за допомогою стеганографічних додатків. Будь-який незвичний зовнішній вигляд у відображенні площини молодшого двійкового розряду буде означати існування вкраплених стеганографічних даних.

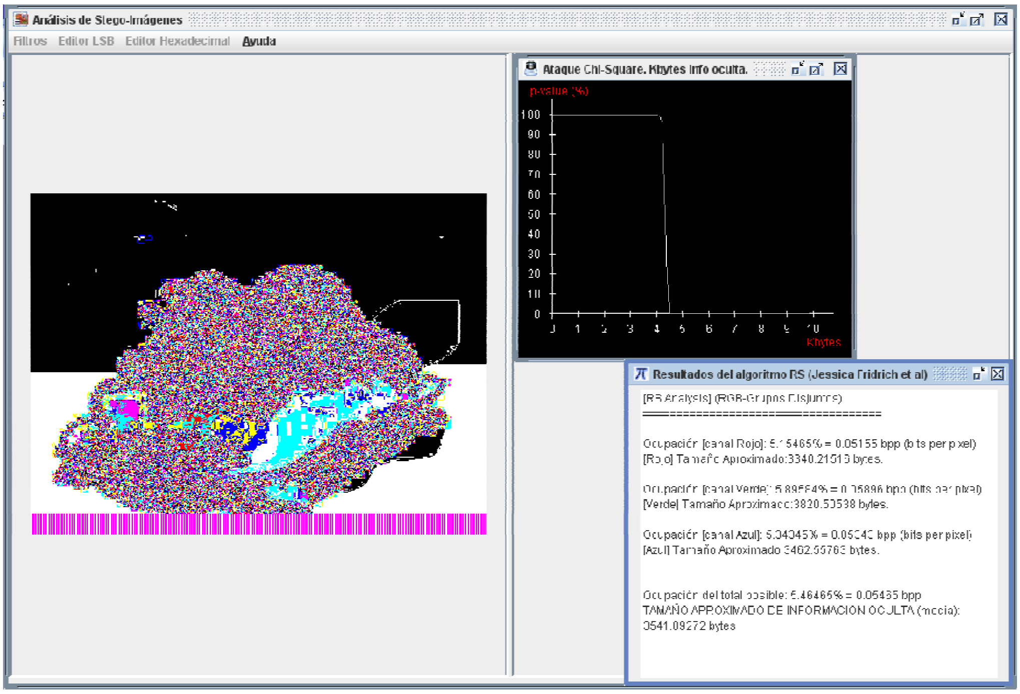


Рисунок 5 – Зовнішній вигляд програми XstegSecret beta v0.1: процедура виявлення інформації в зображенні за допомогою візуального методу бітових площин, методу χ^2 і RS стеганоаналізу

Методи структурного аналізу намагаються виявити зміни у форматі файла даних. Аналіз стеганографічних програм, таких, як Camouflage V1.2.1, appendX v<=4, steganography v1.6.5, DataStash v1.5 показав, що вони «приховують» інформацію, просто дописуючи її в кінець файла-контейнера. Очевидно, подібні програми не є стеганографічними, тому що порушують основні принципи стеганографії – місце розташування, а найчастіше й сама прихована інформація може бути легко виявлена. Програма XstegSecret beta v0.1 надає можливість розпізнати контейнери, до яких прикріплена інформація після мітки кінця файла.

Статистичні методи аналізу намагаються виявити найменші зміни в статистичній поведінці файла, викликаній вкрапленою стеганографією. Відомо, що частоти двох сусідніх елементів контейнера мають перебувати досить далеко від значення частоти середнього арифметичного цих елементів. У «пустому» зображенні ситуація, коли частоти елементів зі значеннями $2N$ і $2N+1$ близькі за значенням, зустрічається досить рідко. При вкрапленні інформації дані частоти зближаються або стають рівними. Ідея методу χ^2 полягає в пошуку цих близьких значень і підрахунку ймовірності вкраплення на основі того, як близько розташовуються значення частот парних і непарних елементів аналізованого контейнера. Результати роботи програми XstegSecret beta v0.1 за критерієм χ^2 залежать від методу, який використовувався при прихову-

ванні інформації. Програма забезпечує гарні результати (рис. 5), якщо приховування інформації здійснювалося за допомогою методу послідовної заміни найменш значущих бітів елементів контейнера або методу вкраплення повідомлення із заповненням. При псевдовипадковому виборі молодших бітів (розподіленому вкрапленні) програма не спрацьовує.

Недоліки:

1. XstegSecret beta v0.1 виявляє біля 40 стеганографічних програм (розпізнає тільки файли *.exe, які використовуються для інсталяції стеганопрограм), але знаходить не всі стеганоконтейнери, які були створені цими програмами.

2. Не дуже зручний інтерфейс для аналізу окремого потенційного файла-контейнера. Доводиться відкривати багато меню, щоб вибрати відповідну опцію.

Останнє оновлення програми було в 2007 році.

Stego Suite

Stego Suite (http://wetstonetech.com/product/stego-suite/) – комерційний програмний продукт, розроблений фахівцями корпорації WetStone Technologies, що спеціалізується на розробці програмних комплексів для гарантування інформаційної безпеки локальних і глобальних комп'ютерних мереж. Замовниками цієї компанії є такі структури, як Військово-повітряні сили США та Національний інститут юстиції.

Програмне забезпечення Stego Suite створено з метою швидкого ідентифікування, дослідження та аналізу цифрових зображень й аудіофайлів на наявність прихованої інформації або секретних каналів зв'язку. Реклама продукту, яка знаходиться на сайті розробника, дає інформацію тільки про його склад і коротку характеристику.

Пакет Stego Suite містить:

– Stego Hunter – програмний компонент, який застосовується для виявлення на досліджуваних файлах-носіях інстальованого або раніше інстальованого стеганографічного програмного забезпечення;

– Stego Watch – програмний інструмент, який сканує всі загальні типи файлів цифрового зображення і аудіофайлів і виявляє будь-які артефакти, використовуючи «сліпий» метод стеганоаналізу.

– Stego Analyst – візуальний аналітичний програмний компонент для всебічного аналізу цифрових зображень й аудіофайлів;

– Stego Break – автоматичний інструмент зламу стеганографічного захисту.

Отримати доступ до комплексу програм можливо з придбанням ліцензії, яка надається за запитом. Вартість ліцензії на офіційному сайті не зазначена.

Недоліки: Неможливість дослідити і проаналізувати програмний продукт.

Steganography Analyzer

Сімейство продукції StegAlyzer створено Центром стеганографічного аналізу й дослідження SARC (Steganography Analysis and Research Center), головним центром в компанії Backbone Security.Com (https://www.sarc-wv.com/). Ці продукти призначені полегшити складну роботу, яка потребує багато часу дослідників під час проведення розслідування, що включає необхідність проведення стеганографічного аналізу.

Steganography Analyzer містить три компоненти: StegAlyzerAS, StegAlyzerSS, StegAlyzerRTS.

StegAlyzerAS – програмний засіб аналізу, який застосовується для виявлення цифрового стеганографічного програмного забезпечення на досліджуваних носіях.

Букви AS у назві програми StegAlyzerAS означають «пошук артефактів» (Artifact Search). Для розпізнання артефактів цифрових стеганографічних додатків відбувається сканування файлової системи, а також реєстру операційної системи Windows.

Щоб визначити, чи існують залишкові файли-артефакти стеганографічних додатків на досліджуваному носії, центр SARC розробив Базу даних контрольних сум стеганографічних додатків (SAFDB – Steganography Application Fingerprint Database). База даних SAFDB містить профілі файлів, пов'язаних з 1025 стеганографічними додатками, додатками для створення цифрових водяних знаків та іншими додатками для приховування даних. Профілі файлів містять ідентифікуючу інформацію, таку як назва асоційованого додатка й кілька унікальних геш-значень: CRC-32, MD5, SHA-1, SHA-224, SHA-256, SHA-384 й SHA-512. Ці геш-значення можуть використовуватися для визначення присутності стеганографічних додатків або артефактів стеганографічних додатків на досліджуваних носіях. База даних SAFDB доступна на сайті центру SARC у форматах, сумісних із програмами Encase, FTK, HashKeeper, ILook, і ProDiscover. База даних SAFDB також поставляється в комплекті із продуктом StegAlyzerAS.

На додаток до геш-значень файлів база SAFDB містить набір ключів реєстру Microsoft Windows® (RAKDB – Registry Artifact Key Database), які створюються або змінюються в результаті інсталяції стеганографічного додатка. Ці значення можна порівняти з досліджуваним реєстром, щоб з'ясувати, чи існував або зараз існує стеганографічний додаток у системі. Якщо є позитивний збіг, то дослідник з високим ступенем ймовірності може стверджувати, що певний стеганографічний додаток існував в аналізованій системі.

StegAlyzerSS (Signature Scanner) – програмний засіб аналізу, що дозволяє переглядати досліджувані файли-носії на присутність шістнадцятирічних послідовностей байтів або сигнатур певних стеганографічних додатків. Після того, як відома сигнатура виявлена, передбачена можливість вилучення інформації, прихованої за допомогою асоційованого додатка. StegAlyzerSS також використовує методи «сліпого» пошуку для встановлення факту наявності прихованої інформації в потенційних файлах-контейнерах.

StegAlyzerRTS – програмний компонент, що виявляє стеганографічні артефакти й сигнатури в мережі в режимі реального часу. Програма визначає завантаження й використання стеганографічних додатків, крадіжку прихованої інформації й спробу відправлення її зовнішнім одержувачам (публікація в Інтернеті, пересилання електронною поштою). Подивитись, як працює ця програма, можна на сайті компанії, переглянувши відеоролик.

На жаль, дослідити, проаналізувати і зробити висновки про якість роботи цих програм не виявляється можливим. Для використання цих програм необхідна ліцензія, яка коштує 995$ для StegAlyzerAS і 1495$ для StegAlyzerSS. Ліцензії включають всі відновлення продуктів протягом одного року з моменту їх придбання.

Недоліки: велика вартість продукту, внаслідок чого неможливий його аналіз.

Висновки

У мережі Інтернет доступні сотні стеганографічних програм, більша їх частина доступна у вигляді безкоштовного або умовно-безкоштовного програмного забезпечення. Ці програми можуть бути використані і в незаконній діяльності. На сьогодні на вітчизняному ринку бракує доступних широкому загалу дослідників і експертів засобів стеганоаналізу, що дозволяють здійснювати контроль використання стеганографічних алгоритмів і припиняти їх нелегальне використання. Актуальною задачею є розробка програмного комплексу, спрямованого на пошук, виявлення і вилучення прихованої інформації.

Література

1. Богуш В.М. Інформаційна безпека від А до Я. 3000 термінів і понять / В.М. Богуш, А.М. Кудін. – К. : МОУ, 1999. – 456 с.
2. Аграновский А.В. Стеганография, цифровые водяные знаки и стеганоанализ / [Аграновский А.В., Балакин А.В., Грибунин В.Г., Сапожников С.А.]. – М. : Вузовская книга, 2009. – 220 с.
3. Швидченко И.В. Методы стеганоанализа для графических файлов / И.В. Швидченко // Искусственный интеллект. – 2010. – № 4. – С. 697-705.
4. Michael T Raggo. Spyhunter: Stegspy [Електронний ресурс] – Режим доступу : www.spy-hunter.com/stegspydownload.htm.
5. Niels Provos. Steganography detection with stegdetect [Електронний ресурс] – Режим доступу : www.outguess.org/detection.php.
6. Provos N. Detecting steganographic content on the internet / N. Provos, P. Honeyman. // Technical Report CITI 01-1a, University of Michigan, 2001.
7. Provos N. Hide and seek: an introduction to steganography / N. Provos, P. Honeyman // IEEE Security Privacy. – 2003. – Vol. 1. – № 3. – P. 32-44. – Режим доступу : http://niels.xtdnet.nl/papers/practical.pdf.

Literatura

1. Bogush V.M. Informacijna bezpeka vid A do Ja. 3000 terminiv i ponjat'. K.: MOU, 1999. 456 s.
2. Agranovskij A.V. Steganografija, cifrovye vodjanye znaki i steganoanaliz. M.: Vuzovskaja kniga. 2009. 220 s.
3. Shvidchenko I.V. Iskusstvennyj intellekt. 2010. № 4. S. 697-705.
4. Michael T Raggo. Spyhunter: Stegspy. www.spy-hunter.com/stegspydownload.htm.
5. Niels Provos. Steganography detection with stegdetect. www.outguess.org/detection.php.
6. Provos N. Technical Report CITI 01-1a. University of Michigan. 2001.
7. Provos N. IEEE Security Privacy. 2003. Vol. 1. № 3. P. 32-44. http://niels.xtdnet.nl/papers/practical.pdf.

RESUME

I.V. Shvidchenko

Investigation of Steganalysis Software

Stegoanalysis is the science about the detection of the fact of hidden data transfer in the analysed cover medium. The detection of hidden data transfer is a complicated process which really needs up-to-date software tools. Nowadays, the wide range of investigators and experts who work in the sphere of data protection lack available software products in steganalysis. The issue of software complex creation, which could include all the known steganalytical methods and the new ones, is one of the most urgent.

The article is devoted to the investigation of steganalysis software, which is currently available on the world software market.

Стаття надійшла до редакції 05.06.2012.